Route Change Latency in Low-Power and Lossy Wireless Networks using RPL and 6LoWPAN Neighbor Discovery

H.R. Kermajani
Wireless Network Group, Entel Dept.,
Technical University of Catalonia (UPC)
Castelldefels, Spain
hrkermajani@entel.upc.edu

C. Gomez
Wireless Network Group, Entel Dept.,
Technical University of Catalonia (UPC)
Castelldefels, Spain
carlesgo@entel.upc.edu

***Abstract*— The IETF ROLL WG is currently in the final steps of the specification of RPL, a new routing protocol for low power and lossy networks (e.g. wireless sensor networks). RPL may use layer two- and layer three-based mechanisms for neighbor reachability maintenance. Since layer two mechanisms may not always be available, RPL relies by default on the 6LoWPAN Neighbor Discovery, a version of the IPv6 Neighbor Discovery which is optimized for LLNs. This paper provides an analysis of the impact of various RPL and 6LoWPAN Neighbor Discovery parameter settings on the link availability and end-to-end path availability, and the related message overhead. Results show that careful tuning of the relevant parameters is critical for obtaining good network performance**.

Keywords-- RPL, 6LoWPAN, Neighbor Discovery, Route Change Latency.

I. INTRODUCTION

In recent years, the Internet Engineering Task Force (IETF) has been developing functionality for extending the Internet to low-power wireless networks, such as wireless sensor networks. This work is a key element for enabling the Internet of Things (IoT) and connecting the next billion nodes to the Internet [10].

One of the work items that are currently being handled by the IETF towards the IoT is the development of an IP-based routing protocol for Low power and Lossy Networks (LLNs). LLNs are composed of devices constrained in terms of battery, memory and processing capabilities. In most LLNs, the devices use low-rate wireless links (wired LLNs are out of the scope of this paper). The IETF Routing Over Low power and Lossy networks (ROLL) Working Group (WG) is currently specifying the IPv6 Routing Protocol for LLNs (RPL) [1].

RPL [1] is being designed taking into account the requirements of control and monitoring applications from many environments, including home and building automation, industrial monitoring, and urban sensor networks. These applications operate in unstable environments, whereby link and node failures may frequently occur (e.g. due to wireless propagation issues, node mobility, changes in the environment, battery depletion, etc.) [11, 12]. In consequence, a radio link may unexpectedly disappear or become unreliable. If that link is being used, then the link failure should be detected and a new route should be used (if any available route exists). This procedure incurs a delay, which has been denoted by Route Change Latency (RCL) [6], that may not be negligible. Nevertheless, timely data transmission is very important for many applications. Some examples are the transmission of medical alarms for users of body medical sensors or pushing a remote control's button in order to perform a command [3].

RPL may use a variety of mechanisms for detecting a link failure, including layer two and layer three mechanisms. The layer two mechanisms may not always be available, and depend on each particular link layer used and are tied to the implementation of RPL for a particular sensor node platform. Hence, RPL relies by default on the layer three protocol called IPv6 Neighbor Discovery (ND) [5]. However, it is expected that LLNs (in particular, those that use radios compatible with IEEE 802.15.4) exploit an optimized version of ND, which is currently being developed by the IETF IPv6 over Low power Wireless Personal Area Networks (6LoWPAN) WG, denoted 6LoWPAN ND [2]. To our best knowledge, the impact of 6LoWPAN ND and the related RPL parameters on network performance has not yet been considered in the literature.

This paper presents a theoretical evaluation of: i) the RCL incurred by RPL when 6LoWPAN ND is used, ii) the impact of the relevant 6LoWPAN ND and RPL parameters on path availability and iii) the trade-off between path availability and message overhead. The remainder of this paper is organized as follows. Section II explains the RPL network model. Section III describes routing in RPL. Section IV focuses on IPv6 ND and 6LoWPAN ND. Section V is devoted to a theoretical analysis of the RCL in RPL and 6LoWPAN ND. Section VI presents a simple analytical model for evaluating end-to-end path connectivity in a network by using RPL and 6LoWPAN ND. Section VII discusses the range of parameters used in the evaluation and Section VIII shows the obtained results. A simple analytical model for calculating the message overhead due to connectivity maintenance is given in section IX. Section X presents the main conclusions.

[1] RPL is pronounced 'Ripple'

II. NETWORK MODEL IN RPL

RPL builds Destination Oriented Directed Acyclic Graphs (DODAGs), based on routing metrics and constraints. A DODAG is a directed graph whereby all edges are oriented in such a way that no cycles exist. The edges are contained in paths oriented towards and terminating at one node that is called the root. The root of a DODAG may act as a sink node in traditional wireless sensor networks, and can be placed in a gateway for providing connectivity to other networks. A set of one or more DODAGs that try to provide a specific objective is named as RPL instance (see Figure 1).

For the construction and maintenance of the DODAG, RPL nodes transmit DODAG Information Object (DIO) messages pseudo-periodically [13]. A DIO message contains information that allows a node to discover a RPL instance, learn its configuration parameters, learn the OF used and maintain the upward routing topology. In addition, the DIO message can include some options. One of these options is the DODAG configuration option, which contains the necessary information to set the parameters in each new node: default lifetime, parameters for scheduling the transmission of DIO messages, etc [1]. Default lifetime specifies the time of validity for all routes in a DODAG. RPL does not currently specify any default value for this parameter.

In order to join a DODAG, a node either can wait to receive DIO messages from nearby nodes or it can send a DODAG Information Solicitation (DIS) to request DIO messages from a subset of neighboring nodes. Each node in a DODAG selects a DODAG parent set, which is composed of the nodes that provide connectivity to the rest of the nodes in the DODAG. For example, in Figure 1, the parent set of node *k* is {*b*, *w*, *u*}. A node uses the Rank property in order to select another node as a DODAG parent. The Rank property is a combination of one or more metrics and constraints into a value. In order to calculate the rank property, the Objective Function (OF) is used. The OF considers some metrics and constraints. Some of these are the following ones: ETX, Latency, HoP-Count (HP), Link Quality Level (LQL), Remaining energy [14].

For data transmission in the DODAG, a member of the DODAG parent set is selected. This node is called the preferred parent and acts as the default router. A node has a set of parents for reliability reasons. Whenever the preferred parent becomes unreachable, the node can select another member of its parent set as preferred parent.

III. ROUTING IN RPL

The core RPL functionality defines two types of routes depending on the direction in which data are transmitted in a DODAG: upward and downward routes. An upward (downward) route provides a path towards (from) the DODAG root from (to) non-root nodes.

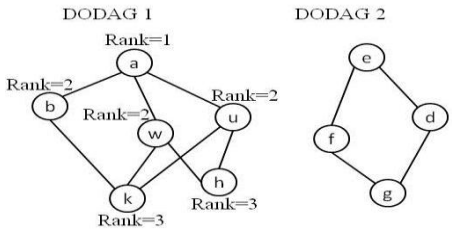

Figure 1. A network with a RPL instance and two DODAGs. Nodes a and e are the roots of DODAG 1 and DODAG 2 respectively.

A. Upward routes

After joining a DODAG, each node learns its upward route(s) by choosing its parent set. Upward routes can be used for data transmission from non-root nodes to the root, i.e. for Multi Point to Point (MP2P) traffic.

B. Downward routes

RPL supports Point to Multipoint (P2MP) traffic, that is, data transmission from the root node to non-root nodes by using the Destination Advertisement Object (DAO) messages. DAO messages are issued by non-root nodes in order to propagate destination information upwards. The next hop destinations to which the node sends DAO messages upward compose the DAO parent set. The DAO message contains various information fields, including the addresses of the DAO sender parents and path lifetime. Path lifetime indicates the period of time during which a destination or a prefix is valid for route determination. Each node is responsible for sending a new DAO message before the expiry of the path lifetime which the node had included in the last DAO. A default value has not yet been proposed for path lifetime in the RPL specification.

RPL defines two modes of operation for downward routing in a DODAG, depending on the storage capabilities of a node: storing and non-storing mode.

1) Storing mode. In the storing mode, all non-root nodes store downward routing tables for their sub-DODAG which contain information obtained from the DAO messages. The sub-DODAG of a node is the set of nodes whose paths to the DODAG root pass through that node. The routing table includes the destination addresses and prefixes along with a node which has a route to these destinations and prefixes, path lifetime, etc. In the storing mode, nodes select the next hop of a downward route by searching a routing table entry for the intended destination address. If there is not a specific entry for the destination in the routing table, the node will pass the packet to its preferred DAO parent by default.

When the metrics and the OF used to select the DODAG parent set and the DAO parent set are the same, these two parent sets are the same.

2) Non-storing mode. In the non-storing mode, nodes do not store routing tables for their sub-DODAG. Instead, nodes downward packets by using source routes populated by a DODAG root.

In both modes of operation when a node either adds a node to its DAO parent set or when it receives a DAO message from its immediate children it should send a DAO

message. In addition, in storing mode, when a node removes another node from its DAO parent set, it has to send a DAO message. In non-storing mode, this is not mandatory. DAO messages are directly sent to the root in non-storing mode and to the DAO parent(s) in storing mode.

C. Point to point routes

In order to transmit data from any node to any other node of the network, RPL supports Point to Point (P2P) flows by using upward and downward routes. In this case, P2P messages first travel up towards the root (which happens in non-storing mode, whereby only the root keeps a routing table for other nodes in the network) or a common ancestor before the root through an upward route. From the root, the messages are then sent towards a destination through a downward route.

RPL also provides one hop communication between any two nodes by using a mechanism based on Multicast Destination Advertisement Messages.

Since the default P2P mechanism used in RPL is not optimal (i.e. there may exist shorter paths than the ones selected by RPL), a reactive mechanism for finding P2P routes is currently being designed [4].

IV. IPV6 AND 6LOWPAN NEIGHBOR DISCOVERY

A. Overview of IPv6 Neighbor Discovery and 6LoWPAN Neighbor Discovery

The IPv6 Neighbor Discovery (ND) [5] has defined a set of important mechanisms for Address Resolution, Duplicate Address Detection, Redirect and Router Discovery along with Prefix and Parameter Discovery for IPv6 networks. However, IPv6 ND is not suitable for LLNs. One reason is the use of multicast signalling, which leads to link layer broadcast in IEEE 802.15.4 networks and consumes excessive energy and bandwidth. Another reason is that IPv6 ND does not support sleeping nodes [2].

In order to solve the problems of IPv6 ND on top of LLNs, the IETF 6LoWPAN WG decided to design an optimized version of the IPv6 ND for LLNs [2] (we refer to this ND version as '6LoWPAN ND'). 6LoWPAN ND is currently still under development [2].

B. 6LoWPAN ND Neighbor Unreachability Detection

In 6LoWPAN ND, each node registers its IPv6 address along with its link layer address in a neighbor cache entry of its default routers. This method is different from the one used in IPv6 ND [5]. In 6LoWPAN ND the address registration can be done by sending a Neighbor Solicitation (NS) message, which in addition to the IPv6 and link layer addresses, includes the node registration lifetime [2]. The receiving router expects that the sending node will be reachable during the registration lifetime specified. After successful registration, the node also expects that the router will be available for the same lifetime. Whenever a node wants to check whether its default routers are still reachable or not, it performs Neighbor Unreachability Detection (NUD). NUD is a mechanism that detects the failure of a neighbor or the failure of the forward path to the neighbor [5].

A node is responsible for maintaining its neighbor cache entries in its routers by performing re-registrations, even when the node does not have data packet to send. Sending data to the router does not serve as a re-registration. In fact, other nodes may want to send data to this node. For this reason, the node repeats sending NS messages to the router periodically before the registration lifetime expiration. In order to save power, sending the NS message for re-registration and NUD can be combined together. In the storing mode of RPL, nodes can use DAO messages instead of NS messages. NUD can only be performed in storing mode, because in non-storing mode, nodes cannot store the addresses of their children in a routing table. Surprisingly, RPL does not currently define any mechanism to detect neighbor unreachability in non-storing mode.

Sending the NS message will be repeated up to MAX_UNICAST_SOLICIT times using a minimum timeout of RETRANS_TIMER until the node receives a Neighbor Advertisement (NA) message from the router in response, or a DAO-ACK if the DAO message has been used in the storing mode of RPL.

The reachability of the router can be acknowledged by using different mechanisms: i) layer two notifications (e.g. by using link layer acknowledgments) or ii) upper layer mechanisms, such as hints from transport layer protocols. However, layer two mechanisms may not always be available. Hence, RPL relies by default on 6LoWPAN ND for neighbor reachability maintenance.

V. RCL WITH RPL AND 6LOWPAN IPV6 ND

In this section we analyze the Route Change Latency (RCL) [6] of RPL and 6LoWPAN ND. For the basis of our study, we consider a simple topology which is shown in Figure 2 (the impact of the RCL on more complex topologies is analyzed in Section VIII). Figure 2.a) illustrates a topology whereby node D is a parent of nodes B and C; node A has selected nodes B and C as its parent set; and node B is the preferred parent of node A. Suppose that node A has registered its address with both of its parents. Then, the AB link fails, which leads to the new network topology depicted in Figure 2.b).

In order to analyze the RCL, we study two different scenarios (see Figure 3). In both scenarios, the last positive confirmation from node B in response to an NS (or DAO) message sent by node A is received at time *T*. Let us assume that node A wants to send a data packet to node D via its preferred parent, node B.

In the first scenario, assume that node B, after sending an acknowledgement to node A becomes immediately unreachable for node A (see Figure 3.a)). In the second scenario, the router unreachability happens right before the registration lifetime expiration (see Figure 3.b). Node A

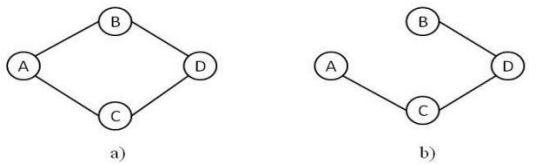

Figure 2. a) Node A has selected nodes B and C as its parents and B is its preferred parent; b) Node B becomes unreachable for node A and subsequently node A selects node C as its preferred parent.

may start sending data to node D at time t_1 because it believes its preferred parent is available during a period of time equal to the registration lifetime indicated in the last NS (or DAO) message sent by node A to node B. The node A will continue data transmission within the registration lifetime duration, until it performs re-registration along with NUD by sending a new NS (or DAO) message to its preferred parent.

We assume that the registration lifetime used in ND is equal to the default lifetime contained in the RPL DIO and path lifetime in DAO messages. For simplicity, we will use the term 'path lifetime' for any of these.

The time required to detect the router unreachability, denoted by T_{NUD}, can be expressed as follows:

$$T_{NUD} = MAX\_UNICAST\_SOLICIT * RETRANS\_TIMER \quad (1)$$

where the MAX_UNICAST_SOLICIT and RETRANS_TIMER parameters are the ones already presented in Section IV. The default values for these parameters are 3, and 1 second, respectively.

If we denote the lifetime of node A by $T_{lifetime}$, the RCL for the first scenario (see Figure 3.a)), can be calculated as follows:

$$RCL = T_{lifetime} + T_{NUD} \quad (2)$$

And for the second scenario (see Figure 3.b)), RCL is equal to:

$$RCL = T_{NUD} \quad (3)$$

Since the router unreachability can occur at any moment within the path lifetime duration, the RCL can be characterized as a uniformly distributed random variable between the two values expressed in equations (2) and (3). Therefore the expected value for *RCL* can be expressed as follows:

$$E[RCL] = \frac{T_{lifetime}}{2} + T_{NUD} \quad (4)$$

VI. END-TO-END CONNECTIVITY MODEL

In this section, we present a simple analytical model to evaluate the impact of using RPL with 6LoWPAN ND on the end-to-end connectivity of an LLN.

We denote the average lifetime of a link, from its creation until the instant in which it disappears, as Time to Link Failure (TLF). We assume that the parent set of all nodes in a DODAG has more than one member. Under this assumption, when a node or link failure occurs in an active path, a node can use another parent as preferred parent to continue the data transmission towards the same destination (note that this is an optimistic assumption). Hence, the probability of link unavailability, which we denote by *q*, can be calculated as follows:

$$q = \frac{E[RCL]}{TLF + E[RCL]} \quad (5)$$

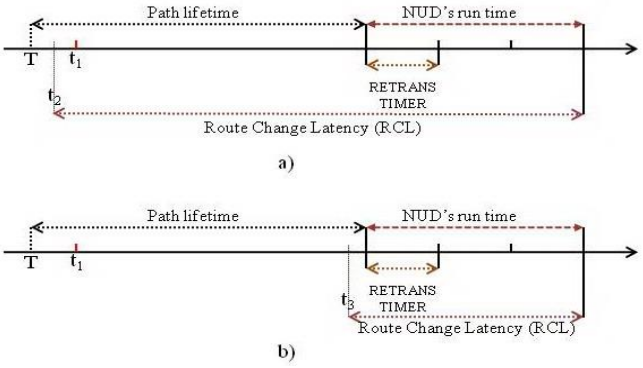

Figure 3. Two scenarios for data transmission and router unreachability. In a) router becomes unreachable right after sending an acknowledgement in response of NS message, at time t2. In b) router unreachability takes place right before the expiration of node's lifetime, at time t_3.

We next calculate the probability of end-to-end path availability for data transmission in a path composed of *N* hops. We have considered that the length of both paths, i.e. the failed path and the new path, is equal to *N*.

Based on these assumptions, and on equation (5), the probability of end-to-end path availability for data transmission in an *N*-hop path, denoted by *P*, is equal to:

$$P = (1 - q)^N \quad (6)$$

VII. DISCUSSION OF TLF AND PATH LENGTH VALUES

This section discusses the TLF and path length range of values for the evaluation of link and end-to-end path availability of an LLN, which is shown in Section VIII.

A. Time to Link Failure

Link failures occur in static scenarios due to phenomena which are intrinsic to radio signal propagation (e.g. multipath, fading, etc.) [12]. Furthermore, changes in the environment that may temporarily attenuate the radio signal (e.g. people moving around, opening and closing a door, rain or snow in an urban LLN) and interference (e.g. from WiFi equipment or from a microwave oven) may affect the reception of radio signals [2, 3]. Link failures may also happen due to node mobility (e.g. due to the mobility of people using on-body sensors or using a portable remote control) and node failures (e.g. due to battery depletion). Depending on the particular environment, the expected TLF may range from less than one minute to more than one day.

B. Number of hops

The expected number of hops in a path depends on each particular scenario and application. For example the number of hops in an industrial application can be up to 20 [9], e.g. when a few hundred nodes are deployed for controlling a very large refinery. In home and building automation [7, 8] the number of hops can be up to 5, whereas for some applications the expected number of hops can be equal to 1 or 2.

VIII. END-TO-END CONNECTIVITY EVALUATION

In order to evaluate the probability of link unavailability and the probability of end-to-end path availability, we consider different configurations for the RPL and

6LoWPAN ND parameters that affect the RCL. These configurations are shown in table Table 1.

The value we use for MAX_UNICAST_SOLICIT for all of these ten configurations (i.e. #1 to #10) is equal to 3, i.e. the default value indicated in 6LoWPAN ND [2]. We believe this value constitutes an appropriate trade-off between reactivity to link failures and spurious link failure detection in a wireless environment.

Note that the RETRANS_TIMER value in configurations #1 to #5 is the default value as proposed in [5]. In configurations #6 to #10 this value is multiplied by 2, in order to compare the impact of this parameter on the probability of end-to-end path availability. We considered as well a RETRANS_TIMER of 0.5 s. However, this setting led to very similar results to those obtained with the default value. Next, we evaluate the probability of link reachability (see Figure 4) and the probability of end-to-end path availability (see Figures 5, 6 and 7) by using equations (5) and (6).

For Figure 4, we have considered the range of TLF values mentioned in Section VII. As shown in Figure 4, all the configurations yield almost 100% link availability for TLF values greater than 5 hours. However, for short-lived links, only the configurations with low path lifetime values offer at least moderate link availability.

For path lifetime greater than or equal to 100 s, results are almost independent of the RETRANS_TIMER setting.

Figures 5, 6 and 7 illustrate the end-to-end path availability for a range of path lengths that covers the various application requirements mentioned in Section VII, and for TLF of 10, 30 and 60 minutes, respectively. For a TLF of 10 minutes, only the configurations that use a path lifetime equal to 10 s offer an end-to-end path availability beyond 70%. When TLF is 30 minutes or 60 minutes, the same end-to-end path availability can be achieved by using a path lifetime of 50 s or 100 s, respectively.

On the other hand, we recommend the use of layer two mechanisms for connectivity maintenance whenever possible, which allow faster reactions to topology changes and better network connectivity. For example, it is possible to detect a link failure in acknowledged IEEE 802.15.4 networks in only 30 ms [15].

IX. NUD MESSAGE OVERHEAD

Using NUD incurs message overhead. A simple analytical model to calculate the rate of NS messages transmitted by a node is as follows:

$$NS\ rate = \frac{(1-q)*1+q*MAX\_UNICAST\_SOLICIT}{Path\ lifetime} \quad (7)$$

where q is the probability of link unavailability (see equation (5)). Figure 8 illustrates the NS message rate for different path lifetime configurations and for different TLF values. We have assumed a RETRANS_TIMER of 1 s (i.e. the default value). As it can be seen, there is a trade-off between the path lifetime and NS message overhead. The path lifetime should be set to a small value in order to increase path connectivity, but on the other hand this will cause a message overhead increase. For TLF values greater than one minute, the NS message overhead curves are the same because the probability of link availability is high.

TABLE 1. PROPOSED PARAMETER CONFIGURATIONS.

Configuration number	Path Lifetime	RETRANS_TIMER (s)
#1	**10**	**1**
#2	**50**	**1**
#3	**100**	**1**
#4	**500**	**1**
#5	**1000**	**1**
#6	**10**	**2**
#7	**50**	**2**
#8	**100**	**2**
#9	**500**	**2**
#10	**1000**	**2**

X. CONCLUSIONS

This paper has provided an analysis of the impact of various RPL and 6LoWPAN ND parameter settings on the link availability, the end-to-end path availability, and the message overhead incurred by RPL and 6LoWPAN ND for connectivity maintenance. Remarkably, important parameters such as default lifetime, path lifetime and registration lifetime do not account with a default proposed value in the related specifications. Results show that careful tuning of the relevant parameters is critical for obtaining good network performance. There is a trade-off between connectivity maintenance and message overhead that depends on the path lifetime parameter. An appropriate configuration of the parameters considered depends on each particular LLN and application. In particular, the parameter choice has to be carried out depending on the expected path length and link lifetime of a scenario.

On the other hand, we recommend the use of layer two mechanisms for detecting link failures whenever possible, since they can be various orders of magnitude faster than layer-three based mechanisms.

ACKNOWLEDGMENT

This work was supported in part by the Spanish Government through project TEC2009-11453.

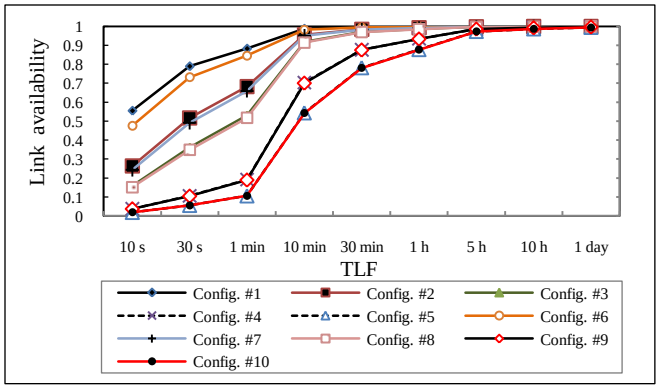

Figure 4. Probability of link availability, using various parameter configurations, for RPL and 6LoWPAN ND.

REFERENCES

[1] T. Winter (Ed.), P. Thubert (Ed.), A. Brandt (Ed.), T. Clausen, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, JP. Vasseur, "RPL: IPv6 Routing Protocol for Low power and Lossy Networks," Internet Draft, draft-ietf-roll-rpl-17, December 2010 (work in progress).

[2] Z. Shelby (Ed.), S. Chakrabarti, E. Nordmark, "Neighbor Discovery Optimization for Low-power and Lossy Networks," Internet Draft, drabi adabft-ietf-6lowpan-nd-15, December 2010 (work in progress).

[3] A. Brandt, J. Buron, G. Porcu, "Home Automation Routing Requirements in Low-Power and Lossy Networks", RFC 5826, April 2010.

[4] M. Goyal (Ed.), E. Baccelli (Ed.), "Reactive Discovery of Point-to-Point Routes in Low Power Networks," Internet Draft, draft-ietf-roll-p2p-rpl-01, October 2010 (work in progress).

[5] T. Narten, E. Nordmark, W. Simpson, and H. Soliman "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, Sep. 2007.

[6] C. Gomez, D. Garcia, J. Paradells, "Improving Performance of a Real Ad-hoc Network by Tuning OLSR", in proceedings of the 10th IEEE Symposium on Computers and Communications (ISCC 2005), 2005.

[7] J. Martocci (Ed.), P. De Mil, N. Riou, W. Vermeylen, "Building Automation Routing Requirements in Low-Power and Lossy Networks", RFC 5867, June 2010.

[8] K. Pister (Ed.), P. Thubert (Ed.), S. Dwars, T. Phinney, " Industrial Routing Requirements in Low-Power and Lossy Networks", RFC 5673, October 2009.

[9] M. Dohler (Ed.), T. Watteyne (Ed.), T. Winter (Ed.), D. Barthel (Ed.), "Routing Requirements for Urban Low-Power and Lossy Networks", RFC 5548, May 2009.

[10] J. Hui, D. Culler, "6LoWPAN: Extending IP to Low-Power, Wireless Personal Area Networks". IEEE Internet Computing, vol. 12, no. 4, pp.37-45, July/August 2008.

[11] A. Woo, T. Tong, and D. Culler,"Taming the underlying challenges of reliable multihop routing in sensor networks", in proc. of SenSys '03, Los Angeles, CA, USA, November 2003

[12] C. Gomez, A. Boix, J. Paradells, "Impact of LQI on the Performance of a One-to-One Routing Protocol for IEEE 802.15.4 Multihop Networks", EURASIP Journal on Wireless Communications and Networking, Volume 2010, Article ID 205407, October 2010.

[13] P. Levis (Ed.), T. Clausen (Ed.), J. Hui (Ed.), O. Gnawali (Ed.), J. Ko(Ed.), "The Trickle Algorithm,"Internet Draft, draft-ietf-roll-trickle-07, January 2011 (work in progress).

[14] JP. Vasseur (Ed.), M. Kim (Ed.), K. Pister, N. Dejean, D. Barthel, "Routing Metrics used for Path Calculation in Low Power and Lossy Networks," Internet Draft, draft-ietf-roll-routing-metrics-16, January 2011 (work in progress).

[15] C. Gomez, P. Salvatella, O. Alonso, J. Paradells, "Adapting AODV for IEEE 802.15.4 Mesh Sensor Networks: Theoretical Discussion and Performance Evaluation in a Real Environment", in proc. of WoWMoM'06, Niagara Falls, June 2006.

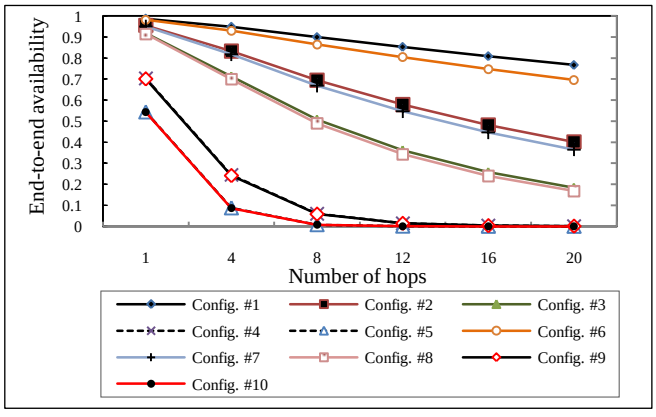

Figure 5. Probability of end-to-end path availability using various parameter settings, for RPL and 6LoWPAN ND, for TLF= 10 Minutes.

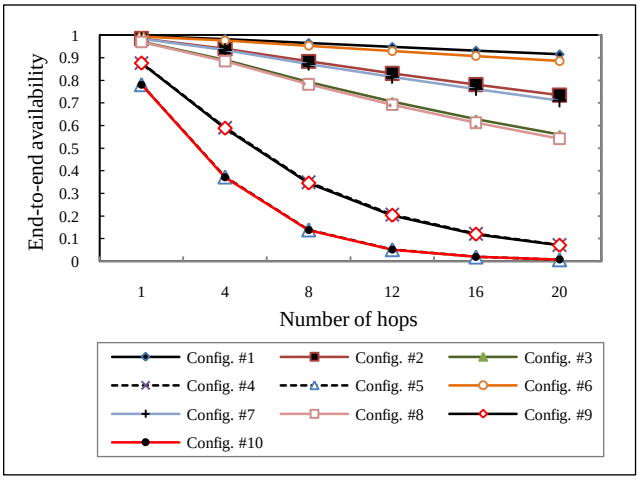

Figure 6. Probability of end-to-end path availability using various parameter settings, for RPL and 6LoWPAN ND, for TLF= 30 Minutes.

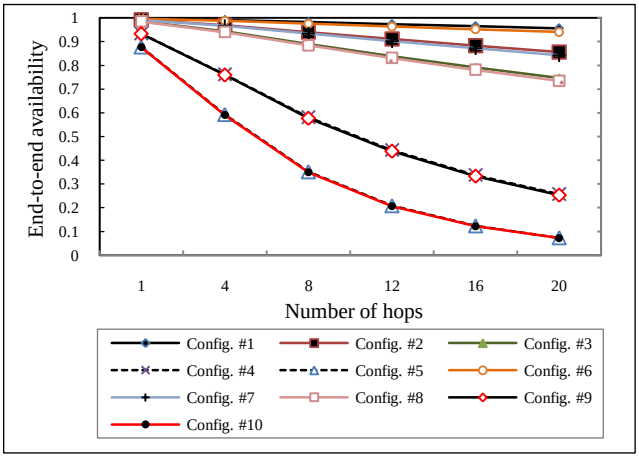

Figure 7. Probability of end-to-end path availability using various parameter settings, for RPL and 6LoWPAN ND, for TLF= 60 Minutes.

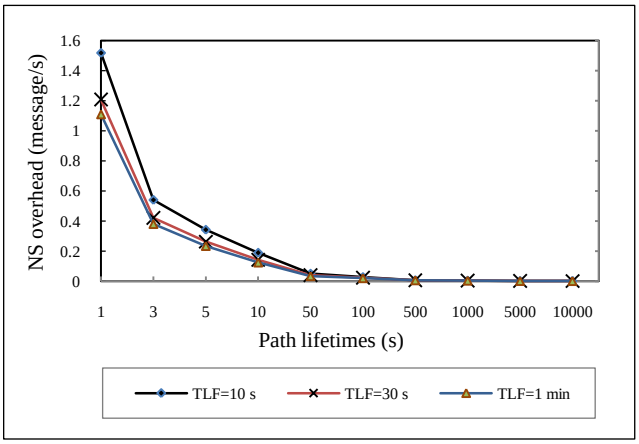

Figure 8. NS message overhead for various path lifetimes.